LISTING OF THE CLAIMS:

1. (Currently Amended) A method ~~for reading in~~ of operating a computer to read-in a password (*p*) upon a request of a program (E), the computer including an operating system having a generator module, the method comprising the steps of:

[-] the generator modules of the operating system, receiving a program-specific identifier (*H(E)*) from said program (E), and receiving said password;

[-] ~~receiving said password (*p*);~~

[-] said generator module generating from at least said program-specific identifier (*H(E)*) and said received password (*p*) a program-password-specific identifier (*F(H(E),p)*); and

[-] sending said program-password specific identifier (*F(H(E),p)*) to said program (E), said program-password specific identifier (*F(H(E),p)*) being processable by said program (E).

2. (Currently Amended) Method according to claim 1, wherein

- the program-specific identifier (*H(E)*) has been derived by applying a first cryptographic function (*H*) to at least part of the code of the program (E), and
- the program-password-specific identifier (*F(H(E),p)*) is generated by applying a second cryptographic function (F) to the program-specific identifier (*H(E)*) and at least part of the

received password (*p*), said first cryptographic function (*H*) and/or said second cryptographic function (*F*) comprising a has function. ~~preferably a one way has function, such as MD5 or SHA-1.~~

3. (Original) Method according to claim 1, wherein a password-reading program (26) and the program-specific identifier (*H(E)*) are provided by means of a trusted computing base (TCB), preferably for both the same trusted computing base (TCB).

4. (Original) Method according to claim 3, wherein the password (*p*) is received at the password-reading program (26), and, while said password-reading program (26) is executed, all I/O devices are locked and other programs are blocked.

5. (Original) Method according to claim 3, wherein the fact that the password-reading program (26) is executed based on the trusted computing base (TCB) is indicated via a signal, preferably illuminating an LED (28), while the password-reading program (26) receives the password (*p*).

6. (Original) Method according to claim 1, wherein the program-specific identifier (*F(H(E),p,s)*) is generated from the program-specific identifier (*H(E)*), the received password (*p*), and an additional value (s), said additional value (s) characterizing a device (2) where the program-password specific identifier (*F(H(E),p,s)*) is generated.

7. (Original) Method according to claim 1, wherein the program-specific identifier (*F(H(E),p)*) is used as a key to decrypt another program.

8. (Original) A computer program comprising program code means for performing the steps of claim 1 when said program is run on a computer.

9. (Original) A computer program product comprising program code means stored on a computer readable medium for performing the method of claim 1 when said program product is run on a computer.

10. (Currently Amended) A computer device (2) for reading-in a password (*p*) upon a request of a program (E) comprising:

an operating system including a generator module;

[-] input means (14) for inputting said password (*p*);

[-] receiver means (26) for receiving a program-specific identifier (*H(E)*) and said password (*p*); and

[-] a said generator-module (22) is connected to said receiver means (26) for receiving said password and said program-specific identifier and for generating a program-password-specific identifier (*F(H(E),p)*) from at least said inputted password (*p*) and said program-specific identifier (*H(E)*), said program-password-specific identifier (*F(H(E),p)*) being processable by said program (E).

11. (Original) The computer device (2) according to claim 10, whereby the generator-module (22) is a has-function generator, and the program-specific identifier (*H(E)*) is derivable from the program (E) by use of said generator-module (22).

12. (Original) The computer device (2) according to claim 10, further comprising a trusted computing base (TCB) and indicator means (28) connected to this trusted computing base (TCB).

13. (Original) The computer device (2) according to claim 12, whereby the indicator means (28) provides a signal that indicates a secure entry mode while a password-reading program (26) provided by said trusted computing base (TCB) is executable.

14. (New) A method according to claim 2, wherein said second cryptographic function is a one-way-has function.